



TITLE:

2次体  $Q(\sqrt{m})$  と  $Q(\sqrt{-m})$  の狭義 ideal 類群の 4-rank の比較(代数的整数論とフェルマーの問題)

AUTHOR(S):

末吉, 豊

---

CITATION:

末吉, 豊. 2次体  $Q(\sqrt{m})$  と  $Q(\sqrt{-m})$  の狭義 ideal 類群の 4-rank の比較(代数的整数論とフェルマーの問題). 数理解析研究所講究録 1996, 971: 134-144

ISSUE DATE:

1996-10

URL:

<http://hdl.handle.net/2433/60692>

RIGHT:

## 2 次体 $\mathbf{Q}(\sqrt{m})$ と $\mathbf{Q}(\sqrt{-m})$ の狭義 ideal 類群の 4-rank の比較

九大数理 末 吉 豊 (Yutaka SUEYOSHI)

### 1 序

$k$  を 2 次体とし,  $C^+(k)$  でその狭義 ideal 類群を表わす. このとき,  $C^+(k)$  の 4-rank  $r_4^+(k)$  は

$$r_4^+(k) = \dim_{\mathbf{Z}/2\mathbf{Z}} C^+(k)_2 \cap C^+(k)^2 = \dim_{\mathbf{Z}/2\mathbf{Z}} \widehat{C^+(k)}_2 \cap \widehat{C^+(k)}^2$$

で与えられる. ここに,  $C^+(k)_2 = \{c \in C^+(k) \mid c^2 = 1\}$  とし,  $\widehat{C^+(k)}$  は  $C^+(k)$  の指標群を表わす. 上の等式の中辺および右辺を計算することにより,  $r_4^+(k)$  についての 2 つの criteria が得られる (Rédei-Reichardt[8], Rédei[7]). 2 つの criteria がいずれも Hilbert 記号を用いて書けることに注意すると,  $m(> 1)$  が平方因子をもたない自然数のとき,  $r_4^+(\mathbf{Q}(\sqrt{m}))$  と  $r_4^+(\mathbf{Q}(\sqrt{-m}))$  の関係を与える "自然な" 単射準同型写像  $\varphi, \psi$  を定義することができる (§3).  $\varphi, \psi$  を用いて, よく知られた不等式

$$r_4^+(\mathbf{Q}(\sqrt{m})) \leq r_4^+(\mathbf{Q}(\sqrt{-m})) \leq r_4^+(\mathbf{Q}(\sqrt{m})) + 1$$

(Damey-Payan[1], Gras[2], Oriat[6], Halter-Koch[3]) の簡単な証明が得られる. また, 等号成立の条件がいろいろな形で書かれ, いくつかの特別な場合に, いずれの等号が成立するかを決定することができる.

### 2 狭義 4-rank についての 2 つの criteria

$d \in \mathbf{Z}$  は,  $d = 1$  または  $d$  が 2 次体の判別式であるとき, 単に判別式とよばれる. 素数  $p$  に対し, 素因数をただ 1 つもつ判別式  $p^* = (-1)^{\frac{p-1}{2}} p$  ( $p$ : 奇素数),  $-4, 8, -8$  ( $p = 2$ ) を素判別式とよぶ.

判別式  $d (\neq 1)$  を固定し,  $k := \mathbf{Q}(\sqrt{d})$  とおく. 判別式  $d_1, d_2$  が  $d = d_1 d_2$  をみたすとき,  $\{d_1, d_2\} (= \{d_2, d_1\})$  を  $d$ -分解とよび,  $S(k)$  で  $d$ -分解全体を表わす.  $m, n (\neq 0) \in \mathbf{Z}$  に対し,  $m \circ n = mn/(m, n)^2$  と定義し,  $\{d_1, d_2\}, \{e_1, e_2\} \in S(k)$  に対し, 積を

$$\{d_1, d_2\} \cdot \{e_1, e_2\} = \{d_1 \circ e_1, d_1 \circ e_2\} \quad (d_1 \circ e_2 = d_2 \circ e_1 \text{ である})$$

で定義すると,  $S(k)$  は elementary abel 2-群となる. 各  $\{d_1, d_2\} \in S(k)$  に対し,  $k$  の狭義  
 不分岐 2 次拡大体  $\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$  が対応するから,  $\dim_{\mathbf{Z}/2\mathbf{Z}} S(k)$  は  $C^+(k)$  の 2-rank  $r_2^+(k)$   
 に等しい.

$D$  が判別式,  $(n, D) = 1$  のとき,  $\left(\frac{D}{n}\right)$  で Kronecker 記号を表わし,  $p$  が素数または  $\infty$   
 で,  $a, b \in \mathbf{Q}^\times$  のとき,  $\left(\frac{a, b}{p}\right)$  で Hilbert 記号を表わす.  $\{d_1, d_2\} \in S(k)$  が第 2 種である  
 とは,

$$\left(\frac{d_2}{p}\right) = 1 \quad (\forall p|d_1) \quad \text{かつ} \quad \left(\frac{d_1}{q}\right) = 1 \quad (\forall q|d_2)$$

をみたすときにいう. この条件は, Hilbert 記号を用いて

$$\left(\frac{d_1, d_2}{p}\right) \left(\frac{d_1, -d}{p}\right) = 1 \quad (\forall p)$$

$$(4||d \text{ のときは更に, } d_1 \equiv 1 \pmod{8} \text{ または } d_2 \equiv 1 \pmod{8}))$$

と書くこともできる. 特に,  $\{d_1, d_2\}$  が第 2 種ならば,  $d_1 > 0$  または  $d_2 > 0$  が成り立つ.  
 $S_2(k)$  で第 2 種  $d$ -分解全体のなす  $S(k)$  の部分群を表わす.

**Rédei-Reichardt criterion**[8, 5]:  $\{d_1, d_2\} \in S(k)$  に対し,

$$\chi_{\{d_1, d_2\}} = \left(\frac{d_1}{\cdot}\right)_2 \left(\frac{d_2}{\cdot}\right)_2 \quad (k \text{ の平方剰余記号}) \in \widehat{C^+(k)}_2$$

とおくと,

$$\chi_{\{d_1, d_2\}} \in \widehat{C^+(k)}^2 \iff \{d_1, d_2\} \in S_2(k).$$

従って,

$$\rho: S_2(k) \longrightarrow \widehat{C^+(k)}_2 \cap \widehat{C^+(k)}^2, \quad \rho(\{d_1, d_2\}) = \chi_{\{d_1, d_2\}}$$

は同型写像で,  $r_4^+(k) = \dim_{\mathbf{Z}/2\mathbf{Z}} S_2(k)$  が成り立つ.

証明.  $d = p_1^* \cdots p_t^*$  を  $d$  の素判別式への分解とし,  $k$  において  $(p_i) = \mathfrak{p}_i^2$  ( $i = 1, \dots, t$ ) と  
 する. このとき,  $C^+(k)_2 = \langle c^+(\mathfrak{p}_1), \dots, c^+(\mathfrak{p}_t) \rangle$  (ただし,  $k$  の ideal  $\mathfrak{a}$  に対し,  $c^+(\mathfrak{a})$  で  $\mathfrak{a}$   
 の属する狭義 ideal 類を表わす) で,  $c^+(\mathfrak{p}_1), \dots, c^+(\mathfrak{p}_t)$  の間に非自明な関係式がただ 1 つ  
 存在する. 従って

$$\begin{aligned}
\chi_{\{d_1, d_2\}} \in \widehat{C^+(k)}^2 &\iff \chi_{\{d_1, d_2\}}(C^+(k)_2) = 1 \\
&\iff \chi_{\{d_1, d_2\}}(\mathbf{p}_i) = \left\{ \begin{array}{l} \left( \frac{d_2}{\mathbf{p}_i} \right)_2 = \left( \frac{d_2}{p_i} \right) (p_i | d_1) \\ \left( \frac{d_1}{\mathbf{p}_i} \right)_2 = \left( \frac{d_1}{p_i} \right) (p_i | d_2) \end{array} \right\} = 1 \quad (i = 1, \dots, t) \\
&\iff \{d_1, d_2\} \in S_2(k).
\end{aligned}$$

□

$d$  の正の約数  $Q$  で平方因子をもたないものの全体を  $D(k)$  で表わす.  $Q_1, Q_2 \in D(k)$  に対し, その積を  $Q_1 \circ Q_2$  と定義すると,  $D(k)$  は elementary abel 2-群である.  $Q \in D(k)$  に対し,  $k$  において  $(Q) = \Omega^2$  とするとき, 全射準同型  $D(k) \ni Q \mapsto c^+(\Omega) \in C^+(k)_2$  が得られ, kernel の位数 = 2. 従って  $r_2^+(k) = \dim_{\mathbf{Z}/2\mathbf{Z}} D(k) - 1 = t - 1$  である.  $n (\neq 0) \in \mathbf{Z}$  に対し,  $[n] \in \mathbf{Z}$  を  $n = [n]a^2$ ,  $a \in \mathbf{Z}$ ,  $[n]$  は平方因子をもたないとして定める.  $Q \in D(k)$  に対し,  $Q' := [Q]d$  とおく.  $Q$  が  $d$ -null divisor であるとは,  $Qx^2 - Q'y^2 - z^2 = 0$  が非自明な有理整数解をもつことと定義する. この条件は

$$\left( \frac{Q, -Q'}{p} \right) \left( = \left( \frac{Q, d}{p} \right) \right) = 1 \quad (\forall p)$$

と同値である.  $D_n(k)$  で  $d$ -null divisors 全体のなす  $D(k)$  の部分群を表わす.

**Rédei's criterion**[7]:  $Q \in D(k)$  が  $k$  において  $(Q) = \Omega^2$  と分解するとき,

$$c^+(\Omega) \in C^+(k)_2 \iff Q \in D_n(k).$$

従って

$$\mu: D_n(k) \longrightarrow C^+(k)_2 \cap C^+(k)^2, \quad \mu(Q) = c^+(\Omega)$$

は全射準同型写像で,  $|\text{Ker } \mu| = 2$ . よって,  $r_4^+(k) = \dim_{\mathbf{Z}/2\mathbf{Z}} D_n(k) - 1$  が成り立つ.

証明. Waterhouse [10], Hasse [4] により簡単な証明が与えられている.  $\chi_i(c^+(\mathbf{a})) := \left( \frac{N\mathbf{a}, d}{p_i} \right)$  ( $i = 1, \dots, t$ ) とおくと,  $\widehat{C^+(k)}_2 = \langle \chi_1, \dots, \chi_t \rangle$  で,  $\chi_1, \dots, \chi_t$  の間に自明でない関係式  $\chi_1 \cdots \chi_t = 1$  (積公式) がただ 1 つ存在する. よって

$$\begin{aligned}
c^+(\Omega) \in C^+(k)^2 &\iff \left( \frac{N\Omega, d}{p_i} \right) = 1 \quad (i = 1, \dots, t) \\
&\iff \left( \frac{Q, -Q'}{p_i} \right) = 1 \quad (i = 1, \dots, t) \\
&\iff Q \in D_n(k).
\end{aligned}$$

□

特に,  $d < 0$  のときは  $-Q' > 0$  だから

$$Q \in D_n(k) \iff -Q' \in D_n(k).$$

このとき,  $\langle Q, -Q' \rangle (= \langle -Q', Q \rangle)$  を  $d$ -null pair とよび, その全体を  $\overline{D}_n(k)$  で表わす.  $\overline{D}_n(k)$  は,  $\langle Q_1, -Q'_1 \rangle \cdot \langle Q_2, -Q'_2 \rangle = \langle Q_1 \circ Q_2, -(Q_1 \circ Q_2)' \rangle$  を積とする elementary abel 2-群で

$$\bar{\mu}: \overline{D}_n(k) \ni \langle Q, -Q' \rangle \mapsto c^+(\Omega) \in C^+(k)_2 \cap C^+(k)^2$$

は同型写像. 従って,  $r_4^+(k) = \dim_{\mathbf{Z}/2\mathbf{Z}} \overline{D}_n(k)$  が成り立つ.

2つの criteria により,  $r_4^+(k)$  の計算はある  $\mathbf{Z}/2\mathbf{Z}$  係数の行列の rank の計算に帰着される (Rédei[7]). 簡単のため,  $\left(\frac{D}{n}\right) = (-1)^a$ ,  $a \in \mathbf{Z}/2\mathbf{Z}$  のとき,  $a = \left(\frac{D}{n}\right)'$  と書く.  $\mathbf{Z}/2\mathbf{Z}$  係数の  $t$  次正方行列  $A_k = (a_{ij})$  を

$$a_{ij} = \begin{cases} \left(\frac{p_i^*}{p_j}\right)' & (i \neq j), \\ \left(\frac{d/p_i^*}{p_i}\right)' & (i = j) \end{cases}$$

で定義する.  $A_k$  のすべての行ベクトルの和は零ベクトルに等しい.  $\mathbf{1} = (1, \dots, 1) \in (\mathbf{Z}/2\mathbf{Z})^t$  とおく.

$$\theta: S_2(k) \longrightarrow \{x \in (\mathbf{Z}/2\mathbf{Z})^t \mid xA_k = \mathbf{0}\} / \{\mathbf{0}, \mathbf{1}\}$$

を  $\theta(\{d_1, d_2\}) = x_{\{d_1, d_2\}} \bmod \{\mathbf{0}, \mathbf{1}\}$ ,  $x_{\{d_1, d_2\}} = (x_1, \dots, x_t) \in (\mathbf{Z}/2\mathbf{Z})^t$ , ただし,

$$x_i = \begin{cases} 1 & (p_i | d_1) \\ 0 & (p_i | d_2) \end{cases} \quad (i = 1, \dots, t)$$

と定義すれば,  $\theta$  は同型写像. 従って

$$r_4^+(k) = \dim_{\mathbf{Z}/2\mathbf{Z}} S_2(k) = t - 1 - \text{rank } A_k.$$

一方,  $A_k$  の第  $t$  列を除いて得られる  $(t-1) \times t$  行列を  $A'_k$  とすると, 平方剰余の相互法則により,

$$\begin{aligned} A'_k &= \begin{pmatrix} \left(\frac{d/p_1^*}{p_1}\right)' & \left(\frac{p_1^*}{p_2}\right)' & \cdots & \left(\frac{p_1^*}{p_{t-1}}\right)' & \left(\frac{p_1^*}{p_t}\right)' \\ \left(\frac{p_2^*}{p_1}\right)' & \left(\frac{d/p_2^*}{p_2}\right)' & \cdots & \left(\frac{p_2^*}{p_{t-1}}\right)' & \left(\frac{p_2^*}{p_t}\right)' \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \left(\frac{p_{t-1}^*}{p_1}\right)' & \left(\frac{p_{t-1}^*}{p_2}\right)' & \cdots & \left(\frac{d/p_{t-1}^*}{p_{t-1}}\right)' & \left(\frac{p_{t-1}^*}{p_t}\right)' \end{pmatrix} \\ &= \begin{pmatrix} \left(\frac{d/p_1^*}{p_1}\right)' & \left(\frac{p_2}{p_1}\right)' & \cdots & \left(\frac{p_{t-1}}{p_1}\right)' & \left(\frac{p_t}{p_1}\right)' \\ \left(\frac{p_1}{p_2}\right)' & \left(\frac{d/p_2^*}{p_2}\right)' & \cdots & \left(\frac{p_{t-1}}{p_2}\right)' & \left(\frac{p_t}{p_2}\right)' \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \left(\frac{p_1}{p_{t-1}}\right)' & \left(\frac{p_2}{p_{t-1}}\right)' & \cdots & \left(\frac{d/p_{t-1}^*}{p_{t-1}}\right)' & \left(\frac{p_t}{p_{t-1}}\right)' \end{pmatrix}. \end{aligned}$$

$Q \in D(k)$  に対し,  $y_Q = {}^t(y_1, \dots, y_t) \in (\mathbf{Z}/2\mathbf{Z})^t$  を

$$y_i = \begin{cases} 1 & (p_i | Q) \\ 0 & (p_i \nmid Q) \end{cases} \quad (i = 1, \dots, t)$$

で定めると,

$$\begin{aligned} A'_k y_Q = 0 &\iff \begin{cases} \left(\frac{Q}{p}\right) = 1 & (\forall p(\neq p_t) | Q'), \\ \left(\frac{\frac{Q}{p} \cdot \frac{d}{p^*}}{p}\right) = 1 & (\forall p(\neq p_t) | Q) \end{cases} \\ &\iff \left(\frac{Q, -Q'}{p}\right) = 1 \quad (\forall p(\neq p_t) | d) \\ &\iff Q \in D_n(k). \end{aligned}$$

従って

$$\theta' : D_n(k) \longrightarrow \{y \in (\mathbf{Z}/2\mathbf{Z})^t \mid A'_k y = 0\}, \quad \theta'(Q) = y_Q$$

も同型写像で、再び

$$r_4^+(k) = \dim_{\mathbf{Z}/2\mathbf{Z}} D_n(k) - 1 = t - 1 - \text{rank } A_k.$$

### 3 狭義 4-ranks の間の関係

$a \in \mathbf{Z}$  に対し,  $d(a)$  により  $\mathbf{Q}(\sqrt{a})$  の判別式を表す. 以下,  $r_4^+(a) = r_4^+(\mathbf{Q}(\sqrt{a}))$ ,  $A_a = A_{\mathbf{Q}(\sqrt{a})}$ ,  $S_2(a) = S_2(\mathbf{Q}(\sqrt{a}))$ ,  $D_n(a) = D_n(\mathbf{Q}(\sqrt{a}))$ ,  $\overline{D}_n(a) = \overline{D}_n(\mathbf{Q}(\sqrt{a}))$  と略記する.

平方因子をもたない自然数  $m(>1)$  を 1 つとり, 固定する.

**命題 1.**  $\varphi: S_2(m) \ni \{d_1, d_2\} \mapsto \langle [d_1], [d_2] \rangle \in \overline{D}_n(-m)$  は単射準同型写像. 従って,  $r_4^+(m) \leq r_4^+(-m)$ .

証明.  $\{d_1, d_2\} \in S_2(m)$  のとき,  $d_1 > 0$ ,  $d_2 > 0$ . 従って,  $[d_1] \in D(-m)$  であって,  $-[d_1]' = -[d_1 \cdot d(-m)] = [d_2]$ . よって

$$\left( \frac{[d_1], -[d_1]'}{p} \right) = \left( \frac{[d_1], [d_2]}{p} \right) = 1 \quad (\forall p).$$

ゆえに,  $\varphi$  は well-defined.  $\varphi$  が単射準同型であることは容易にわかる.  $\square$

**命題 2.**  $\psi: S_2(-m) \ni \{d_1, d_2\} \mapsto [d_1] \in D_n(m)$  (ただし,  $d_1 > 0$  とする) は単射準同型写像. 従って,  $r_4^+(-m) \leq r_4^+(m) + 1$ .

証明.  $\{d_1, d_2\} \in S_2(-m)$  のとき,  $d_1, d_2$  の一方のみ正.  $d_1 > 0$  とすると,  $[d_1] \in D(m)$  で,  $-[d_1]' = [d_2]$ . よって  $\varphi$  の場合と同様に,  $\psi$  も well-defined.  $\psi$  が単射準同型であることも容易にわかる.  $\square$

命題 1, 2 により,  $(\overline{D}_n(-m) : \text{Im } \varphi) \leq 2$ ,  $(D_n(m) : \text{Im } \psi) \leq 2$  もわかる.  $d(m)$ ,  $d(-m)$  を次のように書いておく.

$$\begin{cases} m \equiv 1 \pmod{4} \text{ のとき, } d(m) = p_1^* \cdots p_{t-1}^*, & d(-m) = p_1^* \cdots p_{t-1}^* p_t^*, & p_t^* = -4. \\ m \equiv 2 \pmod{4} \text{ のとき, } d(m) = p_1^* \cdots p_{t-1}^* p_t^*, & d(-m) = p_1^* \cdots p_{t-1}^* (-p_t^*), & p_t^* = 2. \\ m \equiv 3 \pmod{4} \text{ のとき, } d(m) = p_1^* \cdots p_{t-1}^* p_t^*, & d(-m) = p_1^* \cdots p_{t-1}^*, & p_t^* = -4. \end{cases}$$

**定理 1.**  $\text{Im } \varphi$  は次のように書ける.

$$\text{Im } \varphi = \begin{cases} \{ \langle Q, -Q' \rangle \in \overline{D}_n(-m) \mid Q : \text{奇数} \} & (m \equiv 1 \pmod{4}), \\ \{ \langle Q, -Q' \rangle \in \overline{D}_n(-m) \mid Q \equiv 1 \pmod{4} \} & (m \equiv 2 \pmod{4}), \\ \{ \langle Q, -Q' \rangle \in \overline{D}_n(-m) \mid Q \equiv 1 \pmod{8} \} & (m \equiv 3 \pmod{4}). \end{cases}$$

(i)  $m \equiv 1 \pmod{4}$  のとき,

$$\begin{aligned} r_4^+(-m) = r_4^+(m) + 1 &\iff \exists \langle Q, -Q' \rangle \in \overline{D}_n(-m) \text{ s.t. } 2 \mid Q \\ &\iff A_{-m} \text{ の第 } t \text{ 列は他の列の 1 次結合として書ける.} \end{aligned}$$

(ii)  $m \equiv 2 \pmod{4}$  のとき,

$$B_{-m} = \begin{pmatrix} A_{-m} \\ \left(\frac{-1}{p_1}\right)' \cdots \left(\frac{-1}{p_{t-1}}\right)' \left(\frac{-1}{m/2}\right)' \end{pmatrix}$$

とおけば,

$$\begin{aligned} r_4^+(-m) = r_4^+(m) + 1 &\iff \exists \langle Q, -Q' \rangle \in \overline{D}_n(-m) \text{ s.t. } Q \equiv 3 \pmod{4} \\ &\iff \text{rank } B_{-m} = \text{rank } A_{-m} + 1. \end{aligned}$$

(iii)  $m \equiv 3 \pmod{4}$  のとき,

$$C_{-m} = \begin{cases} \begin{pmatrix} A_{-m} \\ \left(\frac{2}{p_1}\right)' \cdots \left(\frac{2}{p_{t-1}}\right)' \end{pmatrix} & (m \equiv 7 \pmod{8}), \\ \begin{pmatrix} A_{-m} \\ \left(\frac{-2}{p_1}\right)' \cdots \left(\frac{-2}{p_{t-1}}\right)' \end{pmatrix} & (m \equiv 3 \pmod{8}) \end{cases}$$

とおけば,

$$\begin{aligned} r_4^+(-m) = r_4^+(m) + 1 &\iff \exists \langle Q, -Q' \rangle \in \overline{D}_n(-m) \text{ s.t. } Q \equiv 5 \pmod{8} \\ &\iff \text{rank } C_{-m} = \text{rank } A_{-m} + 1. \end{aligned}$$

証明.  $\{d_1, d_2\} \in S_2(m)$  とすると,  $d_1 \equiv 1 \pmod{4}$  または  $d_2 \equiv 1 \pmod{4}$ .  $m \equiv 3 \pmod{4}$  のときは更に  $d_1 \equiv 1 \pmod{8}$  または  $d_2 \equiv 1 \pmod{8}$ . また,  $m \equiv 1 \pmod{4}$  のとき,  $\langle Q, -Q' \rangle \in \overline{D}_n(-m)$  において  $Q$  が奇数ならば,  $Q(-Q') = m \equiv 1 \pmod{4}$  および  $\left(\frac{Q, -Q'}{2}\right) \left(= (-1)^{\frac{Q-1}{2} \cdot \frac{-Q'-1}{2}}\right) = 1$  が成り立つから,  $Q \equiv -Q' \equiv 1 \pmod{4}$  となる.



従って,  $\text{Im } \varphi$  は定理に述べた通りとなる.  $r_4^+(-m) = r_4^+(m) + 1$  は  $\text{Im } \varphi \neq \overline{D}_n(-m)$  と同値であるから,  $\text{Im } \varphi$  の形から「 $\exists < Q, -Q' > \in \overline{D}_n(-m)$  s.t.  $\dots$ 」の形の条件と同値であることがわかる. これを行列を用いて書き直せば, 定理にいう条件が得られる.  $\square$

**定理 2.**  $\text{Im } \psi$  は次のように書ける.

$$\text{Im } \psi = \begin{cases} \{Q \in D_n(m) \mid Q \equiv 1 \pmod{8} \text{ 又は } -Q' \equiv 1 \pmod{8}\} & (m \equiv 1 \pmod{4}), \\ \{Q \in D_n(m) \mid Q \equiv 1 \pmod{4} \text{ 又は } -Q' \equiv 1 \pmod{4}\} & (m \equiv 2 \pmod{4}), \\ \{Q \in D_n(m) \mid Q: \text{奇数}\} & (m \equiv 3 \pmod{4}). \end{cases}$$

(i)  $m \equiv 1 \pmod{4}$  のとき,

$$C_m = \begin{cases} \begin{pmatrix} A_m \\ \left(\frac{2}{p_1}\right)' & \dots & \left(\frac{2}{p_{t-1}}\right)' \end{pmatrix} & (m \equiv 1 \pmod{8}), \\ \begin{pmatrix} A_m \\ \left(\frac{-2}{p_1}\right)' & \dots & \left(\frac{-2}{p_{t-1}}\right)' \end{pmatrix} & (m \equiv 5 \pmod{8}) \end{cases}$$

とおけば,

$$\begin{aligned} r_4^+(-m) = r_4^+(m) &\iff \exists Q \in D_n(m) \text{ s.t. } Q \equiv 5 \pmod{8} \text{ または } -Q' \equiv 5 \pmod{8} \\ &\iff \text{rank } C_m = \text{rank } A_m + 1. \end{aligned}$$

(ii)  $m \equiv 2 \pmod{4}$  のとき,

$$B_m = \begin{pmatrix} A_m \\ \left(\frac{-1}{p_1}\right)' & \dots & \left(\frac{-1}{p_{t-1}}\right)' & \left(\frac{-1}{m/2}\right)' + 1 \end{pmatrix}$$

とおけば,

$$\begin{aligned} r_4^+(-m) = r_4^+(m) &\iff \exists Q \in D_n(m) \text{ s.t. } Q \equiv 3 \pmod{4} \text{ または } -Q' \equiv 3 \pmod{4} \\ &\iff \text{rank } B_m = \text{rank } A_m + 1. \end{aligned}$$

(iii)  $m \equiv 3 \pmod{4}$  のとき,

$$\begin{aligned} r_4^+(-m) = r_4^+(m) &\iff \exists Q \in D_n(m) \text{ s.t. } 2|Q \\ &\iff A_m \text{ の第 } t \text{ 列は他の列の } 1 \text{ 次結合として書ける.} \end{aligned}$$

証明. 定理 1 の証明と同様.

$\square$

注 1.  $\varphi, \psi$ を用いた  $r_4^+(m) \leq r_4^+(-m) \leq r_4^+(m) + 1$  の証明は Halter-Koch[3] の証明の改良である. また, 定理 1, 2 で述べた同値条件のうち一部は上原 [9] により得られている. [3] では準同型  $S_2(\pm m) \ni \{d_1, d_2\} \mapsto c(\Omega) \in C(\mathbf{Q}(\sqrt{\mp m}))_2 \cap C(\mathbf{Q}(\sqrt{\mp m}))^2$  (ただし,  $\mathbf{Q}(\sqrt{\mp m})$  において  $(d_1) = \Omega^2$  とし,  $c(\Omega)$  は  $\Omega$  の属する広義 ideal 類を, また,  $C(\mathbf{Q}(\sqrt{\mp m}))$  は  $\mathbf{Q}(\sqrt{\mp m})$  の広義 ideal 類群を表わす) が考察され, [9] では準同型  $S_2(\pm m) \ni \{d_1, d_2\} \mapsto c^+(\Omega) \in C^+(\mathbf{Q}(\sqrt{\mp m}))_2 \cap C^+(\mathbf{Q}(\sqrt{\mp m}))^2$  が考察されている.

系 1. 記号は定理 1, 2 の通りとする.  $m \equiv 1 \pmod{4}$  のとき,  $A_{-m}^*$  で  $A_{-m}$  の第  $t$  列を除いた  $t \times (t-1)$  行列を表わし,  $m \equiv 3 \pmod{4}$  のとき,  $A_m^*$  で  $A_m$  の第  $t$  列を除いた  $t \times (t-1)$  行列を表わす.

- (i)  $m \equiv 1 \pmod{4}$  のとき,  $\text{rank } A_m = \text{rank } A_{-m}^*$ ,  $\text{rank } C_m = \text{rank } A_{-m}$ .
- (ii)  $m \equiv 2 \pmod{4}$  のとき,  $\text{rank } A_m = \text{rank } B_{-m}$ ,  $\text{rank } B_m = \text{rank } A_{-m} + 1$ .
- (iii)  $m \equiv 3 \pmod{4}$  のとき,  $\text{rank } A_m = \text{rank } C_{-m} + 1$ ,  $\text{rank } A_m^* = \text{rank } A_{-m} + 1$ .

注 2. 系 1 より,  $r_4^+(-m)$  と  $r_4^+(m)$  は同時に計算できる. 系 1 の等式は, 行列  $A_{\pm m}$  を直接比較する Gras[2] の第 V 章の方法によっても得られる.

系 2.  $m > 1$  を奇数とする.

(i)  $m$  の素因数がすべて,  $p \equiv \pm 1 \pmod{8}$  をみたすならば,

$$\begin{cases} r_4^+(-2m) = r_4^+(-m) = r_4^+(m) + 1 = r_4^+(2m) & (m \equiv 1 \pmod{8}), \\ r_4^+(-2m) = r_4^+(-m) + 1 = r_4^+(m) + 1 = r_4^+(2m) + 1 & (m \equiv 7 \pmod{8}). \end{cases}$$

(ii)  $m$  の素因数がすべて,  $p \equiv 1$  または  $3 \pmod{8}$  をみたすならば,

$$\begin{cases} r_4^+(-2m) = r_4^+(m) = r_4^+(-m) = r_4^+(2m) & (m \equiv 3 \pmod{8}), \\ r_4^+(-2m) = r_4^+(m) + 1, \quad r_4^+(2m) = r_4^+(-m) & (m \equiv 1 \pmod{8}). \end{cases}$$

証明. 定理 1, 2 の条件を確かめることおよび,  $A_{\pm m}$  と  $A_{\pm 2m}$  の比較により得られる. ここでは, (ii) で  $m \equiv 3 \pmod{8}$  の場合を示す.  $d(m) = p_1^* \cdots p_{t-1}^* p_t^*$ ,  $p_t^* = -4$  とする.

$$\begin{aligned} A_{-2m} &= \begin{pmatrix} * \\ \left(\frac{2}{p_1}\right)' & \cdots & \left(\frac{2}{p_{t-1}}\right)' & \left(\frac{-8m/8}{2}\right)' \end{pmatrix} \\ &= \begin{pmatrix} * \\ \left(\frac{-1}{p_1}\right)' & \cdots & \left(\frac{-1}{p_{t-1}}\right)' & \left(\frac{4m/-4}{2}\right)' \end{pmatrix} = A_m \end{aligned}$$

より,  $r_4^+(-2m) = r_4^+(m)$ . また,  $\text{rank } C_{-m} = \text{rank } A_{-m}$  だから, 定理 1 (iii) より,  $r_4^+(m) = r_4^+(-m)$ . 最後に,

$$A_{2m} = \begin{pmatrix} A_{-m} & * \\ \left(\frac{-2}{p_1}\right)' & \dots & \left(\frac{-2}{p_{t-1}}\right)' & \left(\frac{8m/-8}{2}\right)' \end{pmatrix} = \begin{pmatrix} A_{-m} & * \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

より,  $\text{rank } A_{2m} = \text{rank } A_{-m} + 1$  となって,  $r_4^+(-m) = r_4^+(2m)$ .  $\square$

注 3. 系 2 の等式の一部は上原 [9] により得られている.

上原 [9] と同様の方法により, 次が得られる.

系 3.  $l \in \mathbb{N}$  を奇数とする.

(i)  $m := [l(4l^2 + 1)]$  とおくと,  $m > 1$ . このとき,

$$\begin{cases} l \equiv 1 \pmod{4} \text{ ならば, } m \equiv 1 \pmod{4}, & r_4^+(-m) = r_4^+(m). \\ l \equiv 3 \pmod{4} \text{ ならば, } m \equiv 3 \pmod{4}, & r_4^+(-m) = r_4^+(m) + 1. \end{cases}$$

(ii)  $l > 1$  とし,  $m := [2l(l^2 + 1)] = \left[ l \cdot \frac{l^2 + 1}{2} \right]$  とおくと,  $m > 1$ . このとき,

$$\begin{cases} l \equiv 1 \pmod{4} \text{ ならば, } m \equiv 1 \pmod{4}, & r_4^+(-m) = r_4^+(m) + 1. \\ l \equiv 3 \pmod{4} \text{ ならば, } m \equiv 3 \pmod{4}, & r_4^+(-m) = r_4^+(m). \end{cases}$$

(iii)  $m := [2l(l^2 + 2l + 4)]$  とおくと,  $m \equiv 2 \pmod{4}$ ,  $r_4^+(-m) = r_4^+(m) + 1$ .

(iv)  $m := [2l(l^2 - 2l + 4)]$  とおくと,  $m \equiv 2 \pmod{4}$ ,  $r_4^+(-m) = r_4^+(m)$ .

証明. (i) の  $l \equiv 1 \pmod{4}$  の場合を示す.  $Q := [4l^2 + 1] \in D(m)$  とおくと,  $-Q' = -[l]$ ,  $Q \equiv 5 \pmod{8}$ . また,  $(4l^2 + 1) - 4l = (2l - 1)^2$  より,  $Qx^2 - Q'y^2 - z^2 = 0$  に非自明な整数解が存在する. 従って,  $Q \in D_n(m)$ . よって, 定理 2 (i) より,  $r_4^+(-m) = r_4^+(m)$ . 他の場合も同様.  $\square$

## References

- [1] P. Damey et J.-J. Payan, Existence et construction des extension galoisiennes et non-abéliennes de degré 8 d'un corps de caractéristique différente de 2, J. Reine Angew. Math. 244(1970), 37-54.

- [2] G. Gras, Sur les  $l$ -classes d'idéaux dans les extensions cycliques relatives de degré premier  $l$ , Ann. Inst. Fourier **23**, 4(1973), 1-44.
- [3] F. Halter-Koch, Über den 4-Rank der Klassengruppe quadratischer Zahlkörper, J. Number Theory **19**(1984), 219-227.
- [4] H. Hasse, An algorithm for determining the structure of the 2-Sylow-subgroup of the divisor class group of a quadratic number field, Symposia Math. **15**(1975), 341-352.
- [5] H. Kisilevsky, The Rédei-Reichardt theorem: another proof, Ternary quadratic forms and norms (ed. by O. Taussky), Lecture Notes in Pure Appl. Math. **79**(1982), Marcel Dekker, 1-4.
- [6] B. Oriat, Relations entre les 2-groupes d'idéaux des extensions quadratiques  $k(\sqrt{d})$  et  $k(\sqrt{-d})$ , Ann. Inst. Fourier **27**(1977), 37-60.
- [7] L. Rédei, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, J. Reine Angew. Math. **171**(1934), 55-60.
- [8] L. Rédei und H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, J. Reine Angew. Math. **170**(1933), 69-74.
- [9] T. Uehara, On the 4-rank of the narrow ideal class group of a quadratic field, J. Number Theory **31**(1989), 167-173.
- [10] W. C. Waterhouse, Pieces of eight in class groups of quadratic fields, J. Number Theory **5**(1973), 95-97.
- [11] Y. Sueyoshi, On a comparison of the 4-ranks of the narrow ideal class groups of  $\mathbf{Q}(\sqrt{m})$  and  $\mathbf{Q}(\sqrt{-m})$ , preprint.